Journal of Information Systems Education, Vol. 14(3)

Bitten by a Bug: A Case Study in Malware Infection

Patricia Y. Logan
Marshall University
College of Information Technology and Engineering
Department of Information Systems
100 Angus E. Peyton Drive
Charleston, West Virginia 25303
loganp@marshall.edu

Stephen W. Logan
Weber State University
Department of Information Systems and Technolgies
3804 University Circle
Ogden, Utah 84404-3804
slogan@weber.edu

ABSTRACT

This case study addresses malware infection and the organizational and technical consequences. This case study enables students to view the business continuity issues that should drive all security decisions in IT and allow analysis of the organizational and technical issues that impact recovery from a disaster that is caused by a malware infection. Information systems students seldom see case studies that involve the issues of disaster planning and business continuity within the context of what has become an ever-more frequent occurrence: a virus/worm (malware) infection. This case study would be appropriate for either undergraduate or graduate students in courses involving information resource management, MIS or information security.

Keywords: Virus, malware, information systems management, incident response, disaster planning, business continuity planning

1. INTRODUCTION

Disaster can happen at any time that threatens the continuity of business activities and does not have to be from a physical disaster, such as an earthquake or hurricane. Increasingly, the availability and reliability of networks and infrastructure has been compromised by malware: viruses, worms, and Trojans designed to impact network and employee productivity. Malware represents the deliberate and malicious release of software that is designed to impact the productivity and profitability of individuals and corporations. ICSA Labs reports that from every 1,000 computers, the infection rate will be 105. A disaster is defined as simultaneous attack on 25 or more computers or an attack causing major damage. The impact of downtime (defined as a significant loss of availability and reliability of networks, hardware or software) equates to lost revenue and increased expenses. As many sales, manufacturing, administrative, and production functions are automated and depend on networks for access, the unrecoverable loss of data can close a business, permanently. Contingency Planning Research (2000) estimates the cost per one hour of downtime for various industries in Figure1 (http://www.ontrack.co.uk/datarecovery/cost.asp). It is estimated that only 6 per cent of companies suffering from a catastrophic data loss survive the business disruption. The loss worldwide to malware is not trivial: the

Figure 1
The Cost of Downtime

Type of Industry	Cost per Hour
Retail Brokerage	$6.45 million
Credit card sales authorization	$2.6 million
Infomercial or 800-number promotions	$199,500
Catalog Sales centers	$90,000
Airline reservations	$85,000
ATM service	$14,000

legendary Love Bug cost $9.63 billion, the leading virus in 2002, Klez with $9.9 billion, Code Red cost $2.89 billion, and the most recent SQL Slammer is estimated to cost $1 billion (MI2g).

Less obvious in terms of loss is the productivity of employees that depend on computers for operations, customer support, plus loss of opportunities in missed sales and customer satisfaction. A business continuity plan can prepare for the unexpected interruption of computer operations. Ideally, this plan should include the eventuality of a malware infection that disrupts operations for a significant period of time. ICSA labs surveyed firms with more than 500 computers and found that the time to recover from each virus disaster in 2002 was 23 days. Seventy-five per cent of those surveyed had a significant virus outbreak and 62% had critical files corrupted by malicious programs. A plan should outline the activities of the IT organization, the recovery and work-arounds for all impacted business units in order to quickly resume operations. With the cost of malware clean-up estimated by ICSA to be $81,000, the need for a plan to minimize losses is a critical component of over-all business strategy.

Disaster by malware is most often found to have email as the locus of infection with 86% of all malware traced to email attachments. The first line of defense against malware disasters has been anti-virus software that can detect viruses, worms, and Trojans in email attachments. Despite the presence of anti-virus software, companies continue to experience infections; in fact most of the last major infections occurred despite adequate anti-virus protection. Chris Belthoff, a senior security analyst at antivirus software maker Sophos, worries about the eventual impact: He thinks such worm attacks are turning e-mail into "such a polluted protocol that it's quickly becoming unusable from a business perspective."

Virus writers have been prolific in exploiting the vulnerabilities in desktop and server operating systems creating malware that by passes anti-virus products. A virus writer summarized the issue of vulnerabilities, ” Some of these vulnerabilities have been known for years and the biggest of them has been known for centuries; Human Stupidity” (Delio). Virus writers use social engineering techniques to deliver their virus and ensure that the damaging payloads are delivered. Companies often do not include in their continuity plans a provision for adequate training of employees in understanding the social engineering that is used as a component by virus writers of their plan to deliver the virus to the company. Malware has become more sophisticated, with the creation of blended threats: a threat that spreads like a worm as well as an email virus making it harder to control and to get rid of.

The following case describes a hypothetical incident. In reading thiscase keep in mind that this company believed that they were adequately prepared against malware disaster because they had installed an anti-virus product on the desktops and servers. Hundreds of computers were infected with a stealth virus not recognized by the latest antivirus software. The primary network at its U.S. headquarters had been shut down at 10 a.m., when the desktop support manager realized there was no other way to stop the virus from spreading. The virus, BadBoy, was on a rampage—copying itself to other systems and shutting machines down.

2. CASE OVERVIEW

Logan Industries, is a multi-national catalog sale corporation with offices in 30 states, 3 countries, and has 2,600 employees. The CEO is Andrew James, a man committed to technology and known throughout the company as a technology buff. The company has a frame relay WAN (wide area network) connecting all offices, and each office has its own Windows 2000 server. The home office is located in California, where the IT department staff reside. While most offices are small, with fewer than 50 employees, the home office has the bulk of the operations and sales staff numbering 600 employees. The IT department is led by Ms. Pamela Lau, the CIO. She has an IT manager, Jim Smythe, who directs the IT operations. The infrastructure consists of servers, high-speed fiber backbone, switching technology, desktops running Windows 2000 and an anti-virus product on all servers and desktops. Jim Smythe is challenged to manage a network and desktops that are spread throughout the nation and relies on out-sourcing technical support in regional areas to service the computing needs of many staff. Additionally, he sends on a quarterly basis a team of his desktop and network support staff to the larger U.S. and international offices. Ms. Janis Moto is the help desk manager and is the point of contact for employees that need support or service for their desktop.

3. THE VIRUS ATTACKS

3.1 First Infection: Monday, Feb. 5

In 2003, 20 employees at a satellite sales office received an email from the CEO and President Andrew James with the message:

> From: Andy.Smith@Logan.com
> Subject: From the President
>
> Hi!
>
> I just had to send you this plug-in for our quarterly sales spreadsheet. Our email server won’t let me email programs so I’ve renamed it. Save it to disk, changing the .app at the end to .exe, then you can run it. I don’t normally forward this kind of thing, but this will really impress you!
>
> Take care,
>
> Attachment:  Plug_in.app

Shortly after receiving the email, employees followed the directions and downloaded the attached file renaming it to their C: drive and/or network share. Twenty employees experienced a computer shut-down a short time later. Attempts at rebooting sent them into an endless reboot loop. A desktop support technician, visiting the office on other business, looked at a couple of the misbehaving computers and identified symptoms typical of a virus. To stop it from spreading, she told the infected users to log off the network and wait for the help desk to contact them about fixing their machines. The support technician let the help desk know about the problem and figured that the help desk would tell employees to update their virus definition files.

3.2 The Virus Spreads: Tuesday, Feb. 6

Early in the morning, the infection had spread from dozens of computers to hundreds. The virus appeared to have mailed itself to everyone in the Outlook address book. Unknown to the IT staff, the virus scanned the email outbox looking for the last ten people emailed with attachments. The virus parsed the message responding as if a follow-up with the phrase, "I sent you XYZ file but forgot to add this attachment". After sending itself, it would cause the machine to reboot and never to recover.

The IT desktop staff examined one of the infected computers and found code in the registry identifying the virus as BadBoy. The staff emailed instructions for everyone to look for BadBoy, the virus that was not yet recognized by the latest version of antivirus software. Anyone who found it was to call the help desk. At the help desk, the phone wouldn't stop ringing.

By 10 a.m., the CIO had been called and decided to form a team to deal with the virus. Two hours later, the team had decided on a leader and authorized a shut-down of the network to contain the virus. That meant no email for U.S. employees, no remote access for mobile users, no connection to offices in other countries, and no communication with stores, which could still ring sales and process credit card transactions but could not look up customer data or inventory at other locations.

By noon, when the virus team realized how damaging the virus was, they told everyone at headquarters to turn off their computers. The only exceptions were 50 employees on a secondary network that hadn't been infected running critical programs on the AS400 mainframe, which controlled shipping and inventory.

An IT desktop support member had found some of the virus's Visual Basic code with the header, "A clever virus by Dark Sam written in the year 2003." They emailed the code to the anti-virus vendor's research lab. This research team discovered that BadBoy was a network-aware worm that spreads through email to users in the Microsoft Outlook address book. When a user executes the infected file, the virus adds itself to the startup folders and places the plug-in.exe file in the start-up path. It attempted to copy itself to the following network shares:

C$\windows\startup\plug-in.exe
C$\WINNT|Profiles\All Users\Start Menu\Programs\Startup\plug-in.exe
C$\Documents and Settings\All Users\Start Menu\Programs\Startup\plug-ins.exe

Team members were desperate to hear from the anti-virus vendor's help desk. The IT manager called the help desk and demanded to speak with a manager, who said the company needed to wait 24 hours for a response.

The CIO called the local police who referred her to the FBI. At first, the person who answered the phone at the FBI wasn't sure if the case fell under the bureau's domain, and asked the CIO to substantiate the dollar loss and amount of damage. The CIO knew there was lost business, and possibly more than $5,000 damage. Stores were affected in more than one state. The FBI started building a case, in hopes of bringing the perpetrator to trial with enough damage to make a prosecution worthwhile. They asked for samples of code to begin looking for clues as to the identity of the virus writer.

3.3 Late Afternoon: Wednesday, February, 7th

Wednesday afternoon, the AV developers sent a first attempt to find BadBoy on the disk drive and clean any infected files. The "fix" found the virus but destroyed some critical operating system files. Disheartened, the team came up with step two of what would be called the "temp fix": a way to clean the hard disk of the plug_in.exe. Technicians used a text search utility that works in DOS, to search for a text string that identified BadBoy. When they found the virus, they spent from five to 10 minutes manually removing the virus code from all file locations. The team of technicians visited each desktop, marking each one with a green sticker to indicate that the machine was "fixed", and also began locating and cleaning infected files on the email and file servers at the home office.

Users at Logan Industries had now been without access to a computer for three days and were getting frustrated. The help desk was unable to broadcast when the virus infection would end and connectivity would be restored. The sales manager seeing his quarterly bonus disappearing with the failure to close a couple of big sales locked himself in his office to use his laptop despite the warnings by the team not to use any computers on the infected network. He subsequently infected his laptop and a server that had been "cleaned" of the virus.

The AV vendor's attempts to detect, clean and fix what the virus had done were getting better. By Friday afternoon, they sent a fix that both identified and removed the virus. IT team skipped the rest of the homegrown manual clean and began focusing on the remainder of the computers. Desktop support technicians spent the rest of Friday, all day Saturday and half of Sunday returning to all 600 PCs

in the home office. This time, they taped signs to all "cleaned" computers warning users not to power up until they got the OK. No plan was yet in place to deal with the other offices at distant locations. They decided to meet later that day to plan the how to repair the remaining hardware.

4. THE NEXT WEEK: RECOVERY

Monday morning at 10 a.m., the intercom in the home office finally blared good news: Employees could use their computers again. Stores could now communicate. European and U.S. locations could now communicate. (European locations, which were warned about the virus by fax, only had a few infections.).

For IT, however, the war wasn't over. A dozen computers in the home office were so corrupted that the technicians needed to completely reinstall the operating systems and applications. There were details to take care of with the servers, remote office locations (with 1,500 infected desktops), and 500 mobile users who needed to overnight their laptops to headquarters for fixing. The loss of some critical data files impacted the sales staff and efforts would begin to attempt recovery from back-up devices.

5. THE CONSEQUENCES

The CEO requested a report from the CIO. The report included the following costs:

Incident Costs

Item	Hours	Cost/Hr	Total
Incident Investigators (team)	150	$15.68	$2,352
System Administrator (team)	200	$25.00	$5,000
Consultant	200	$24.95	$20,000
Staff	200	$15.00	$3,000
Subtotal	750		$30,352
Benefits @ 28%			$10,352
Subtotal (Salary and Benefits)			$40,704
Industry Avg. Downtime/Hour	200	$90,000	$18,000,000
Cost			**$18,040,704**

The CIO and CEO had no idea how to value the lost productivity for over 2,000 employees or to calculate the loss in sales when communication with customers and suppliers was cut for a week. The FBI pursued the lead provided by the IT department and contacted DaRkSaM. He took full credit for "BadBoy" but defended himself, saying he only writes and publishes viruses on the Internet and couldn't prevent others from downloading and releasing them into the wild. He wrote in an email to the investigating FBI agent from the safety of his home in Europe that, "Better that you find out about a hole in your operation through my virus than through some unethical hacker smashing into your machines and stealing all your so-called private data." For DaRkSaM, it was an issue of free speech and performing a community service. In his view it was not negligence but a charitable donation of time to provide assistance to businesses.

6. CONCLUSION

The learning objectives for this case comprise the following:

- The ability to describe the business impact of virus/worm infection
- A comprehension of the responsibilities of an IT staff in delivering a secure environment
- The steps to respond to and recover from a malware infection
- Enumeration of the threats posed by a malware infection

Downtime is not just an IT nuisance but a significant factor in the loss of sales, drop in stock prices and damage to reputation. The impact of a network outage reaches to all devices that are attached to the network: email, web, file, database, print servers, as well as desktop and remote employees use of laptops. Malware is a low risk and high payoff activity for an attacker. Hackers are assisted in their efforts by the naiveté of most users and the absence of a comprehensive security plan that offers training to users in the recognition and response to malware received in the guise of harmless email.

7. REFERENCES

http://www.icsalabs.com/
http://www.contingencyplanningresearch.com/
http://www.businessweek.com/technology/content/aug2003/tc20030826_4386_tc047.htm
http://www.ontrack.co.uk/datarecovery/cost.asp

AUTHOR BIOGRAPHIES

Patricia Y. Logan is an associate professor at Weber State University in the Goddard School of Business and Economics (currently on leave). She is teaching at Marshall University in the College of Information Technology and Engineering within the Department of Information Systems for the academic year 2003-2004. She has worked in the field of information technology management for over fifteen years. Dr. Logan held senior IT management positions in the banking and insurance industries. Her primary teaching responsibilities include computer forensics and information security

Stephen W. Logan is an instructor in information systems and technologies at Weber State University. He has worked as a software developer and analyst and taught a variety of software development courses. His primary teaching responsibilities include information technology for business and software development using Visual Basic and VB.net.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096